U.S. Department of Homeland Security
Washington, DC 20229

U.S. Customs and
Border Protection

NOV 2 4 2008

MEMORANDUM FOR: (b) (6), (b) (7)(C)
Deputy Secretary
Department of Hon(b) (6), (b) (7)(C)

THROUGH: (b) (6), (b) (7)(C)
Chief, U.S. Border Patrol

FROM: (b) (6), (b) (7)(C)(b) (6), (b) (7)(C)
Executive Director, Secure Border Initiative (SBI)

SUBJECT: SBI*net* Operational Requirements Document (ORD) Elements Applicable to Block One System

REFERENCE: SBI*net* ORD Version 1.0 dated March 6, 2007

This memorandum provides Block 1 allocated requirements to the ORD as required by the Acquisition Decision Memorandum dated September 8, 2008.

Block 1 is the first increment of a spiral development effort. Subsequent blocks will be developed through an evolutionary process that identifies capabilities gaps required to achieve border control, supports analysis of alternatives and supports the development and delivery of capability enhancements to the operators.

Attachment (1) is a complete list of ORD Block 1 requirements. ORD Block 1 requirements for testing at (b) (7)(E) are indicated. Also specified are requirements that will be deferred to later Block 1.x deployments. Block 1 deferred requirements will allow continued research and development of deferred systems by the prime contractor. All Block 1 requirements are a subset of the original requirements found in the referenced document. Operational requirements from referenced document remain unchanged.

Attachment (2) specifies modified Key Performance Parameters (KPP) applicable for Block 1 systems. Modified KPPs contain supporting descriptive information that was lacking in referenced document and better align with Block 1 allocations.

Attachments: (1) Table of Applicable Block 1 Operational Requirements from ORD version 1, dated March 6, 2007

(2) Block 1 KPP

Attachment 1: Table of Applicable Block 1 Requirements

The table below specified the requirements listed in Section E of the ORD that apply to Block 1 systems. In addition to these requirements, Section C of the ORD specifies system architectural philosophy. All elements listed in the ORD section C apply to Block 1 systems with the exception of C.8 Intelligence Requirements. Intelligence integration will occur in Block 2 deployments and later. In addition, SBI*net* shall integrate with legacy system specified in Section A, especially Remote Video Surveillance Systems (RVSS) and Mobile Suveillance Systems (MSS) during Block 1.x.

Reference	Requirement Statement	(b) (7)(E) Testing at	Block 1.x (Deferred)
E.3.1.1	The system shall provide surveillance coverage tailored to the operational environment with consideration given to (b) (7)(E) (b) (7)(E) to best support the detection and characterization or classification of items of interest. This includes:	X	
E.3.1.1.2	(b) (7)(E)	X	
E.3.1.2	The system shall positively and accurately detect items of interest in the vicinity of the border, in both directions. (Also see Section F KPPs)	X	
E.3.1.3	The system shall positively and accurately identify and classify items of interest in the vicinity of the border, in both directions. (Also see Section F KPPs)	X	
E.3.1.4	Surveillance assets shall operate 24 hours per day, in all-environmental conditions, and in all geographic areas to detect and classify items of interests.	X	
E.3.1.5	The system shall enable continuous coverage or provide the capability to repeatedly visit the same objects, areas, items of interest with the same, different, or a combination of sensors.	X	
E.3.1.5.1	The surveillance assets (when used in combination) shall provide continuous coverage through data fusion and correlation.	X	
E.3.1.6	Surveillance assets shall have the capability to interoperate.	X	
E.3.1.7	Mobile detection shall be provided to support CBP enforcement personnel with identifying the following items:		
E.3.1.7.1	(b) (7)(E)		X
E.3.1.7.2			X
E.3.1.7.3			X
E.3.1.7.4			X
E.3.1.7.8			X
E.3.1.9	Surveillance assets shall allow for complete coverage of the specified area or zone to be surveilled.	X	
E.3.1.11	The system surveillance asset shall provide the capability to detect and identify multiple simultaneous events with different individuals or groups.	X	

Attachment 1: Table of Applicable Block 1 Requirements

Reference	Requirement Statement	(b) (7)(E) Testing at	Block 1.x (Deferred)
E.3.1.14	The system shall provide the ability to monitor surveillance effectiveness.	X	
E.3.3.1	The system shall allow command center staff the capability to (b) (7)(E) (b) (7)(E)	X	
E.3.3.2	The system shall identify the source of recorded transactions.	X	
E.3.3.3	(b) (5)		X
E.3.3.4	The system shall provide the capability to store and retrieve information:		
E.3.3.4.1	(b) (7)(E)	X	
E.3.3.4.2	– Indefinately in archive system	X	
E.3.3.4.3	– Can be electronically retrieved on demand	X	
E.3.3.4.4	– Information stored that is not SBI-specific or SBI-generated shall comply with the "system of record" policies for the system from which the information came.	X	
E.3.3.5	(b) (7)(E)		X
E.3.3.6	The system shall completely and accurately transmit data.	X	
E.3.3.7	Communications transfer shall eliminate the potential for information to be received or transmitted by personnel without proper authorization.	X	
E.3.3.8	(b) (7)(E)		X
E.3.4.1	(b) (7)(E)		
E.3.4.1.2			X
E.3.4.2	(b) (7)(E)	X	
E.3.4.3	The system shall provide event/incident status tracking capability.	X	
E.3.4.4	(b) (7)(E)		X
E.3.4.5	(b) (7)(E)		
E.3.4.5.1		X	
E.3.4.5.2		X	
E.3.4.6	(b) (7)(E)		
E.3.4.6.1			X
E.3.4.6.2			X

Attachment 1: Table of Applicable Block 1 Requirements

Reference	Requirement Statement	(b) (7)(E) Testing at	Block 1.x (Deferred)
E.3.4.7	(b) (7)(E)		X
E.3.4.8			X
E.3.4.9	The system shall provide the capability for the user to customize the display of information that is provided to them with regard to the size of a display from one visual image (b) (7)(E)	X	
E.3.4.11	The system shall provide an integrated picture capability for selected data sources.	X	
E.3.4.15	(b) (7)(E)		
E.3.4.15.1			X
E.3.4.15.2			X
E.3.4.15.3			X
E.3.4.15.4			X
E.3.4.15.5			X
E.3.4.15.6			X
E.3.4.21	The system shall provide the capability to status the item of interest from detection through resolution.	X	
E.3.4.22	(b) (7)(E)		X
E.3.4.24	The system shall provide CBP enforcement personnel capability to input event data	X	
E.3.4.25	The system shall display the (b) (7)(E) e status and resolution of items of interest	X	
E.3.5.1	The system shall receive and provide location and operational status of supporting assets within the designated area of responsibility to include but not limited to the following:		
E.3.5.1.1	– Command center computing resources	X	
E.3.5.1.2	– SBI*net* surveillance assets	X	
E.3.5.1.3	(b) (7)(E)		X
E.3.5.1.4			X
E.3.5.1.5			X
E.3.5.2	The system shall provide the capability to visually represent location and operational status information.	X	
E.3.6.1	SBI*net* operating system services shall provide the capability to encrypt law enforcement sensitive data upon transmitting or storing it per DHS and CBP standards.	X	
E.3.6.2	SBI*net* operating system services shall provide the capability for an authorized administrator to manage the methods, keys, and mechanisms it uses.	X	

Attachment 1: Table of Applicable Block 1 Requirements

Reference	Requirement Statement	(b) (7)(E) Testing at	Block 1.x (Deferred)
E.3.6.3	(b) (7)(E)	X	
E.3.6.4	The system shall provide identification, authentication, and access control capabilities that conform to DHS system security access standards to include DHS policy contained in DHS 4300A – Sensitive Systems Policy and Handbook, and DHS Security Architecture Guidance Volumes 1 through 3.	X	
E.3.6.5	System design shall support and integrate with (b) (7)(E) (b) (7)(E)	X	
E.3.6.7	The system shall utilize appropriate security measures that align with current DHS and CBP technical architecture profile standards.	X	
E.3.6.8	(b) (7)(E)		X
E.3.6.9	SBI*net* operating system services shall be capable of controlling and limiting access to system resources via (b) (7)(E)	X	
E.3.6.10	SBI*net* operating system services must protect passwords (b) (7)(E) (b) (7)(E)	X	
E.3.6.12	The system shall provide identification, authentication, and access control capabilities using a secure operating system.	X	
E.3.6.15	(b) (7)(E)	X	
E.3.7.1	SBI*net* operating system services shall provide an audit capability and maintain an audit trail of all events.	X	
E.3.7.2	SBI*net* operating system services shall provide tools for searching, sorting, and printing audit trail contents.	X	
E.3.7.3	SBI*net* shall store audit events for future use.	X	
E.3.7.4	The system shall provide the capability to audit all recorded transactions and events occurring within the system to include but not limited to an audit of:		
E.3.7.4.1	– Recorded transactions by an individual surveillance asset	X	
E.3.7.4.2	– Transactions between components.	X	
E.3.7.4.3	– Database actions	X	
E.3.7.4.4	– User actions to identify who was doing what on the system and when they	X	
E.3.7.4.5	– (b) (7)(E)		X
E.3.7.4.6	–		X
E.3.7.4.7	The system shall provide an open system design that promotes the following:	X	
E.3.7.4.7.1	– Modularity	X	

Attachment 1: Table of Applicable Block 1 Requirements

Reference	Requirement Statement	(b) (7)(E) Testing	Block 1.x (Deferred)
E.3.7.4.7.2	– Reconfigurability	X	
E.3.7.4.7.3	– (b) (7)(E)		X
E.3.7.4.7.4	– Scalability	X	
E.3.7.4.7.5	– Upgradeability	X	
E.3.8.1	System information required to affect CBP enforcement personnel response shall be provided in (b) (7)(E) .	X	
E.3.8.2	(b) (7)(E)		
E.3.8.2.1			X
E.3.8.2.4			X
E.3.8.3			X
E.3.8.4			X
E.3.8.5			X
E.3.8.6	The system shall permit multiple computing operations (b) (7)(E) l.	X	
E.3.8.7	Definition and selection of the minimum configuration for desktop computer software, application and database, and hardware configuration for computers shall be dependent on the performance requirements necessary to meet the mission and will comply with the DHS TRM.	X	
E.3.8.8	Voice and data communications between system nodes shall be protected appropriately based on risk and sensitivity.	X	
E.3.8.9	Performance of communications components shall function with high reliability under reasonably foreseeable circumstances.	X	
E.3.8.11	Implementation shall reliably provide the appropriate power and bandwidth at the least cost that will support the demand.	X	
E.3.8.12	Surveillance assets shall have the capability to be remotely programmable to support changes in the operational environment.	X	
E.3.8.14	SBI*net* operating system services shall appropriately allocate and clear the contents of a storage object before assigning resources to another process.	X	
E.3.8.15	The system shall provide the capability to measure, collect, and report network performance metrics.	X	
E.3.8.16	The system shall provide the capability to measure, collect, and report sensor performance metrics.	X	
E.3.8.17	The system shall provide the capability to initiate automated fault notification of designated assets, correlate corrective action until resolved, and archive the information.	X	
E.3.8.18	(b) (7)(E)	X	
E.3.8.19	(b) (7)(E)		X

Attachment 1: Table of Applicable Block 1 Requirements

Reference	Requirement Statement	(b) (7)(E) Testing at	Block 1.x (Deferred)
E.3.8.22	The system shall provide the capability to remotely troubleshoot and perform software upgrades to communication and sensory devices.	X	
E.3.8.24	(b) (7)(E)		X
E.3.10.1	System implementation and deployment shall comply with federal, state, and local environmental guidelines for the location where the system is employed and the type surveillance asset used.	X	
E.3.10.4	(b) (7)(E)	X	
E.3.10.5	(b) (7)(E)		X
E.3.10.6			X
E.3.10.7	The system shall provide the operations center the capability to enter aliases for map features.	X	
E.3.10.8	The system shall provide specific identifying physical markings on towers as visual landmarks and for collision avoidance for aircraft.	X	

F. Key Performance Parameters

Section F presents SBI*net* Key Performance Parameters (KPP) identified as the program's critical essential characteristics or capabilities. Failure to verify these capabilities through acceptance and other system testing could result in program reassessment, delayed initial operating capability, or contract termination.

A performance parameter's threshold is the minimum value necessary to provide an operational capability that will satisfy the requirement. A performance objective is a value beyond the threshold that should reflect an operationally meaningful, measurable, cost-effective, affordable, impact on operations or support beyond that provided by the threshold value. In some cases the threshold and objective may have the same value.

F.1	Probability of IoI Detection[1]	Probability of IoI Detection = # Actual IoI Detections / # Actual IoIs in the AOI	(b) (7)(E)
F.2	Probability of Correct Identification[2]	$P_{Identification}$ = # Correct IoI Identification Events / # Possible IoI Identification Events	
F.3	Operational Availability[3]	A_O = Uptime / Uptime + Downtime	

Notes:

1. Probability of IoI Detection:
   a. Standard test procedure is to measure in a controlled test environment with the:

(b) (7)(E)

   b. Probability IoI detected estimates may be estimated in an operational environment using operational statistics including, but not limited to: (b) (7)(E) apprehension statistics, and station COP user statistics.

2. Probability of Correct Identification:
   a. IoIs are identified (b) (7)(E)
   b. Standard test procedure is to measure on an operational range and determined by direct measurement at event end, or time of CBP agent intercept. This entails

correct identification (b) (7)(E)

(b) (7)(E)

3. Operational Availability:
    a. Operational Availability (A_o): The degree (expressed as a decimal between 0 and 1, or the percentage equivalent) to which one can expect a piece of equipment or weapon system to work properly when it is required. It is the quantitative link between readiness objectives and supportability. It can also be calculated by the number of systems that are ready, divided by the number possessed (e.g., the number of times the system was available, divided by the number of times the system was required) for on-demand systems.